Messaging and Server COIN

October 24, 2006

Agenda

- Server Functional Area Status
  - Transformation Lab
  - HP OpenView
  - Server Consolidation
  - Other
  - Timeline
- Platforms & Images High Level Design
- Virtualization Infrastructure High Level Design
- Messaging High Level Design Review
- Active Directory High Level Design Review
- Questions
- Next Meeting Topics

Server Functional Area

Agenda

- Server Functional Area Status
  - Transformation Lab
  - HP OpenView
  - Server Consolidation
  - Other
  - Timeline
- Platforms & Images High Level Design
- Virtualization Infrastructure High Level Design

NORTHROP GRUMMAN

Server Functional Area

Status Update

Transformation Lab Status

- Obtained VITA Architecture Review (VAR) approval
- Received and assembled hardware
- Loaded operating systems
- Built lab Steady State environment
- Installed ESX virtual infrastructure
- Installed Messaging environment

HP OpenView Status

- Obtained VAR approval
- Installed HPOV servers on network monitoring subnet
- Installed Network Node Manager (NNM)
- Loaded hosts (selected network devices and servers)
- Standing up Temporary Network Operations Center (TNOC) and Interim Infrastructure Operations Center (IIOC) to monitor up/down status of selected network devices and servers

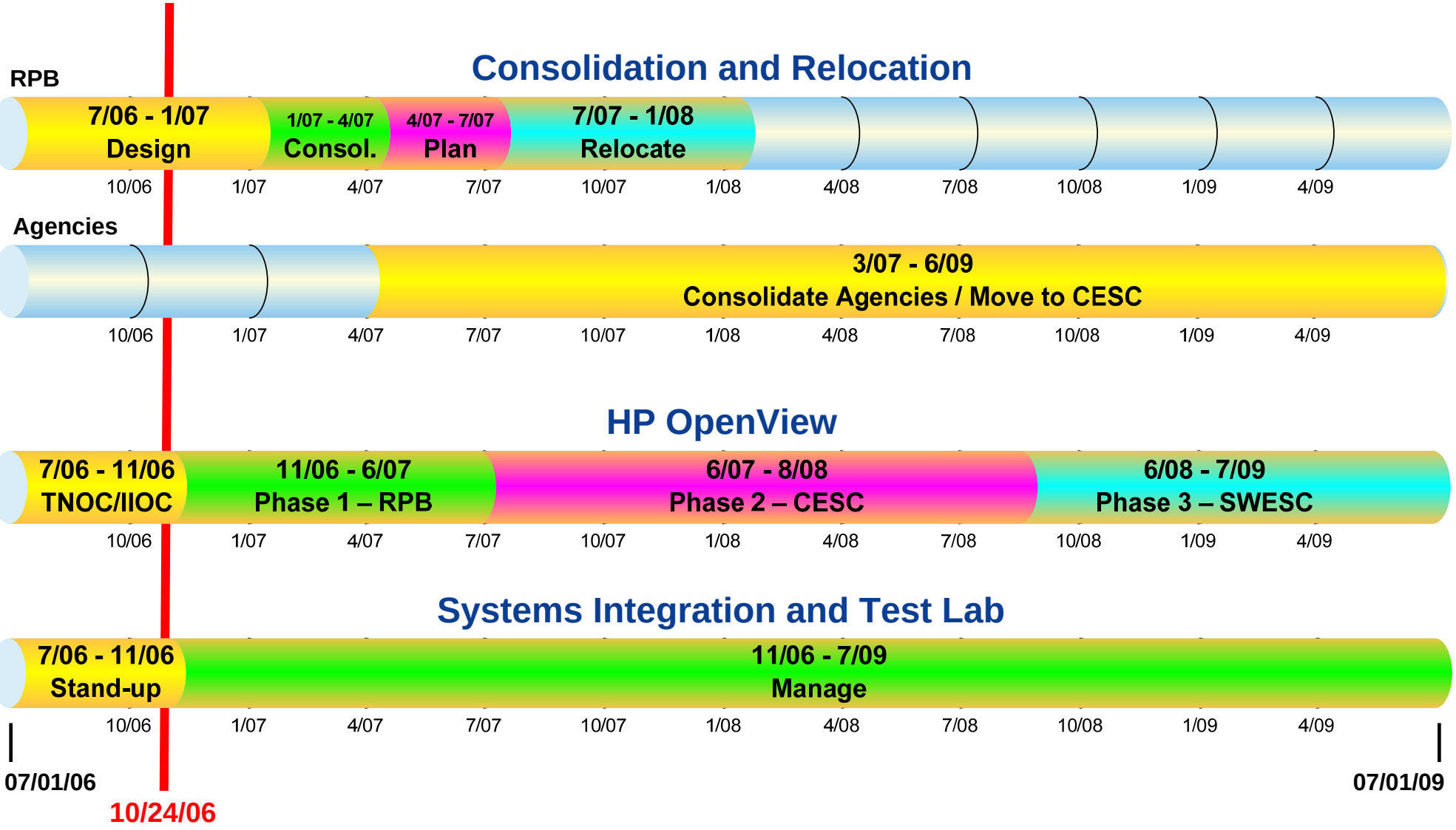
Server Consolidation Status

- Designing End-State Environment:
  - Hardware configurations
  - Operating system images
  - Virtual, Citrix, File and Print Infrastructures
- Rationalizing inventory of servers in RPB
- Perform server discovery and identify consolidation candidates beginning in RPB in November, 2006
- Begin server consolidation in RPB in January, 2007

Other Status

- Beginning to develop schedules for consolidating servers in the Greater Richmond Area and beyond
- Evaluating standard Wintel and UNIX hardware vendors

Server Functional Area Timeline



Platform & Images

High Level Design

General Description

- As in most IT industry segments:
  - Across all agencies, systems from almost all major vendors (and white-box) are installed
  - Almost all Operating Systems with multiple versions are installed
  - Multiple x86 hardware platforms (models and vendors) are represented

Overall Solution Description

- Introducing standard platform and OS images provides a means to simplify the server infrastructure
  - Standard hardware configurations provides a means of significantly reducing the number of vendors and models within the VITA environment
  - Standard OS configurations provides a means of significantly reducing the number of operating systems and versions
  - Standard base operating system images provides a means of standard OS and common components across the VITA environment

Overall Solution Description

- x86/x64 Standard Platforms
  - Rackmount Servers – mid and high-end
  - Blade Servers – mid and high-end
- Unix servers
- Standard Operating Systems
  - Microsoft
  - Linux
  - HP-UX

Overall Solution Description

- Storage
  - Redundant 4 Gb Fibre Channel HBA's across two paths
  - Local mirrored OS and swap
  - Applications & Data on SANBlade Enclosures
- Blade Enclosures
  - 2 x GigE Network Switches
  - 2 x 4Gb SAN Switches
- Racks
  - One KVM (Keyboard, Video, Mouse) for 16 units
  - Redundant power supplies
  - 220 volt power
- Network
  - Redundant 4 x GigE ports across two hardware paths
  - Dedicated out-of-band management port

Standard Images

- Windows 2003 Standard Server
- Windows 2003 Enterprise Server
- Redhat Linux AS
- Redhat Linux ES
- HP-UX 11i
- VMware 3.0 infrastructure
- Windows 2000

Suggested OS Image Parameters

- OS Disk
  - 2 x 73GB Mirrored
- Data / Application disks
  - Any number of 10 GB & 50 GB LUNs
  - Larger sizes created via OS utilities
- Management & Monitoring
  - OpenView Operations
  - Altiris
  - Other
- Backup tool
  - NGC/VITA selected tool
- Anti-Virus Software
  - Symantec (x86)
- HBA Failover Software
  - Storage vendor-specific tools (x86)
  - OS based solution (Unix)
- Ethernet Redundancy
  - Teamed Gigabit adapters

Virtualization Infrastructure

High Level Design

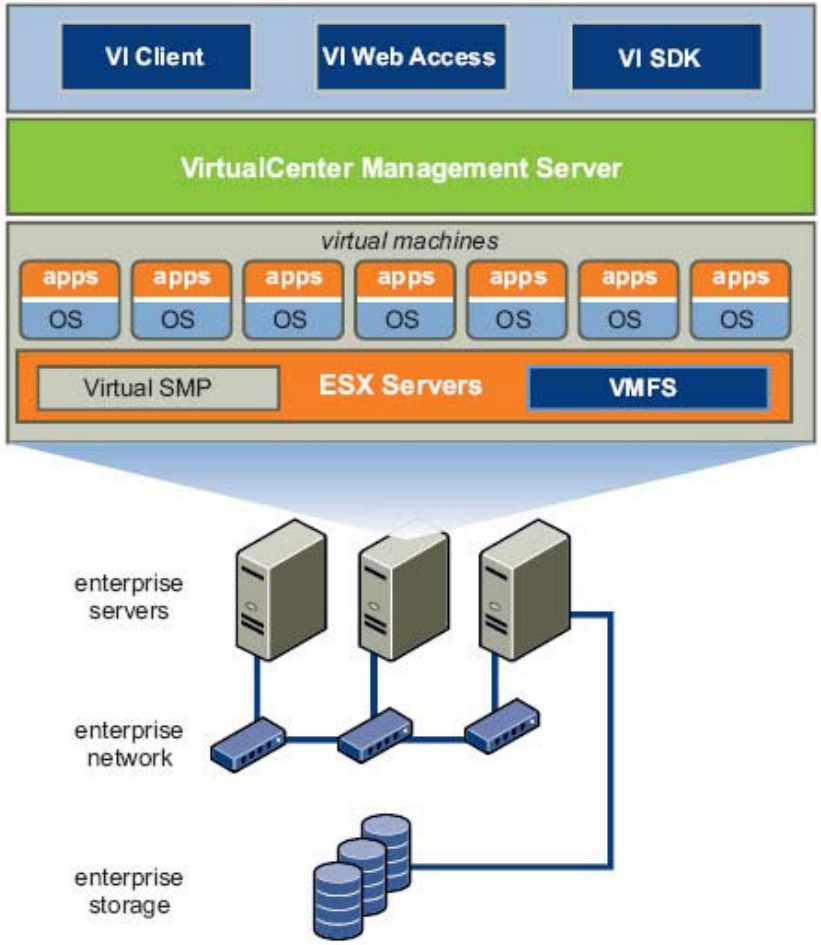
General Description

- As in most IT industry segments:
  - Across all agencies, average x86 server utilization is expected to be below 10%
  - Datacenter floor space, power, and cooling are significant limiting factors
  - Lack of consistency in x86/x64 platforms increases complexity of infrastructure management
  - Networking infrastructure is growing at an alarming rate, also with very low utilization rates
  - Raw storage capacity is growing at an exponential rate, with significant amounts of “captured storage”

Overall Solution Description

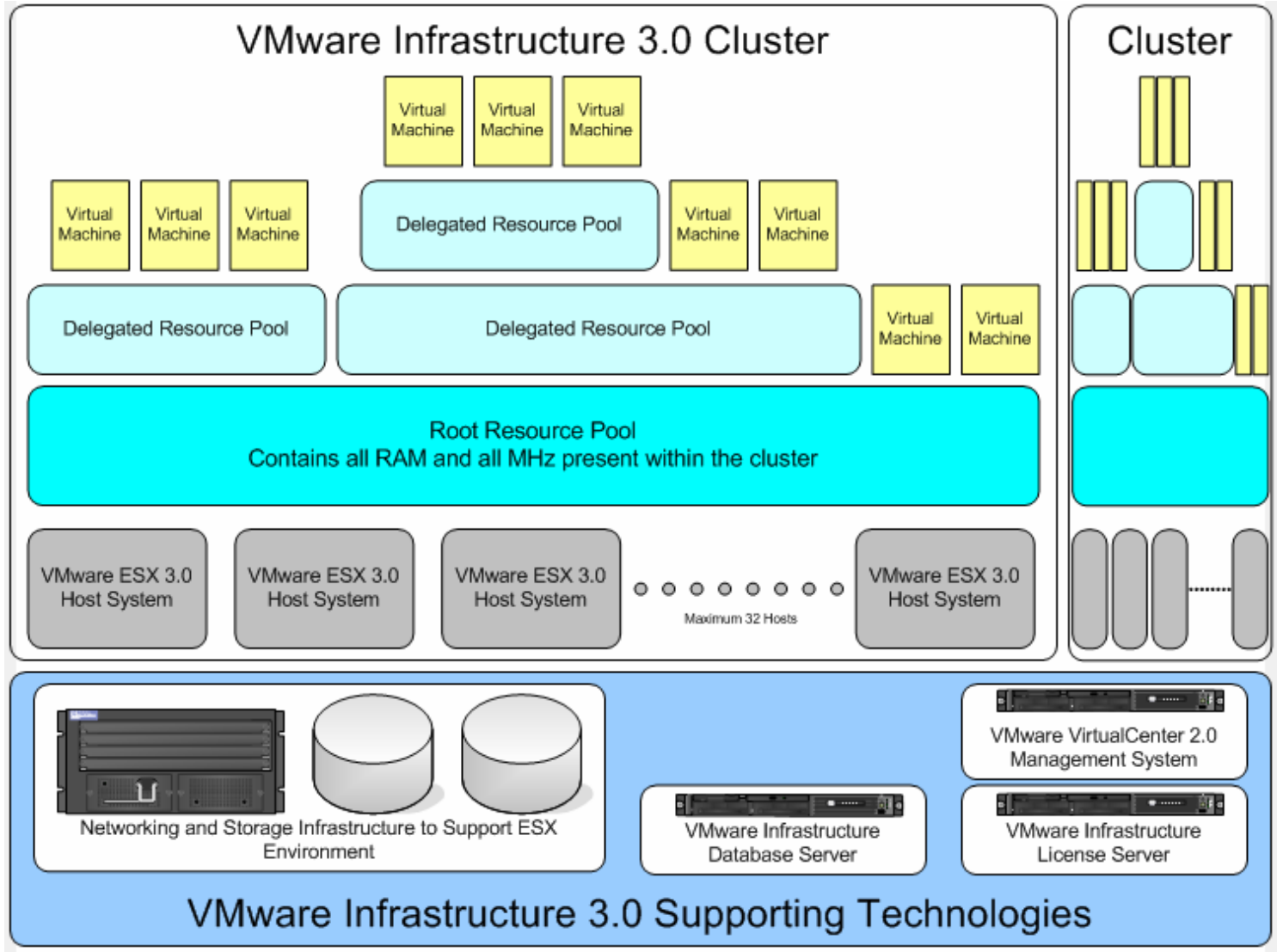
- Server virtualization provides a means to significantly reduce the number of physical servers in the VITA environment
- The VITA virtual environment will utilize VMware Infrastructure 3 (VI-3) to provide the virtual platform
- VMware ESX Server 3
  - Virtualization Host
- VMware VirtualCenter 2
  - Centralized management of virtual infrastructure
  - VMware VMotion

VMware Infrastructure Components



- VMware Infrastructure 3
  - VMware ESX Server 3
  - VMware VirtualCenter 2
    - Centralized Management
    - VMware VMotion
  - FlexNet License Server
    - Can use existing license server
    - Limited version bundled with VI-3
  - VirtualCenter Database Server

VMware Infrastructure Overview



Virtual Infrastructure Composition

- Dedicate physical server for use as VirtualCenter platform
- Use existing VITA database resources for VirtualCenter datastore
- Use existing or bundled FlexNet license server
- VI-3 clusters will be comprised of identical physical servers whose number will be determined after testing in the Lab.
- VI-3 clusters will be provisioned with enough capacity to support the failure of or removal of a number of hosts that will be determined after testing in the Lab.
- Capacity expansion achieved by adding additional clusters rather than by extending existing clusters

Implementation Plan

- Use virtual infrastructure to support migration of existing workloads from physical servers to virtual machines (P2V)
- Virtualize in Place (ViP) where feasible and then migrate to CESC
  - Uses standardized virtual infrastructure hardware configuration
  - Reduces risk by isolating transformation phases
    - Virtualization
    - Change of IP address

Storage

- Each VI-3 host connected to Fibrechannel SAN storage
  - Redundant 4Gbps Fibrechannel HBA
- LUNs sized to support storage needs of 20 notional VMs
  - Assume 20GB / VM = 400GB LUNs
  - Other sizes by exception
  - Formatted as VMware File System (VMFS) volumes
- VMFS volumes use a standardized naming/labeling convention

Backup / Restore

- Backup / Restore performed identically to physical systems
  - Backup network isolated by VLAN
  - Each VM configured with second virtual NIC to connect to backup network
  - Backup agent installed in guest OS
- ESX servers not backed up
  - No important configuration files stored locally
  - Use automated server provisioning to deploy newly configured server

Provisioning

- ESX hosts provisioned via Altiris toolset
- Virtual Machines provisioned via Altiris toolset
  - Virtual Machines are identified as VITA standard hardware platform
  - Will require a customized image

Enterprise Management

- VMware VirtualCenter
- Deploy/Include Enterprise Management agent in VM image
- Deploy/Include Enterprise Management agent in ESX host installation script

Operational Impact

- End Users
  - Minimal impact – outage during virtualization
- Application Administrators
  - Minimal impact
- System Administrators
  - Simplified management
- Virtual Infrastructure Admin
  - New administrative role responsible for ensuring availability of Virtual Infrastructure

Questions?

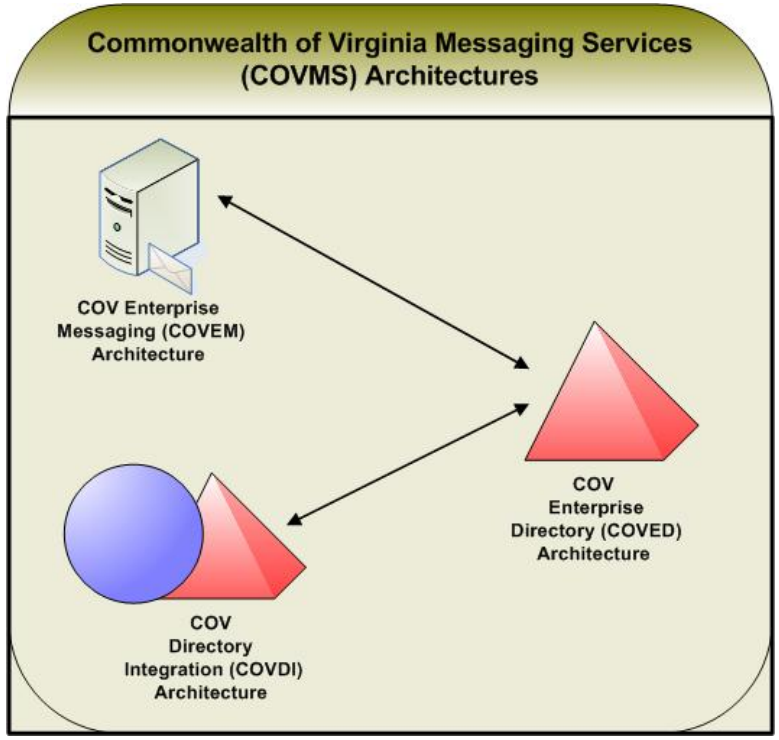
Messaging
High Level Design Review

Agenda

- Introduction
- Current Environment
- Requirements and Vision for Exchange and Adjunct Services
- Timeline and Transformation Phases
- Solution Overview
  - High Level Design Elements
  - Hardware / Software Systems
  - Interface to Existing Solutions
  - User Interaction
  - Dependencies

Introduction

Messaging Tower Tracks:



- **Exchange – Messaging and Adjunct Services (Blackberry, LCS, Unified Messaging, Fax, etc.)**
- Directory Synchronization – MIIS, LDSU, and other products provide a common GAL and a unique identifier for users. Also lays the groundwork that would be necessary to support other services in the future (TBD)
- Active Directory – Windows 2003 AD to provide an enterprise directory, single source for authentication, etc. Also, DNS, WINS, and related services
- Migration – how are users and mailboxes in agency directories and email systems going to transition to the new messaging infrastructure?

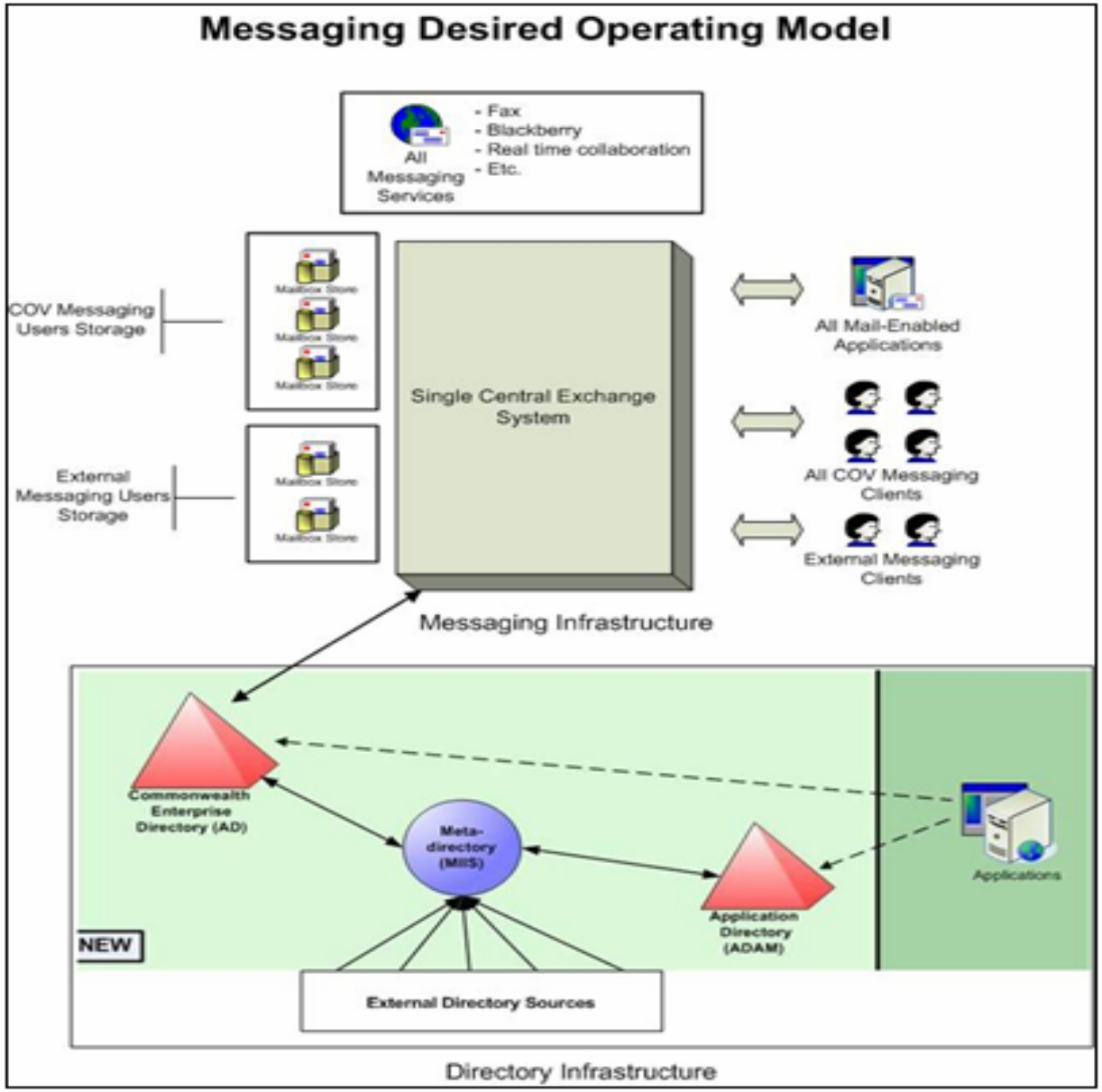
Current Environment

- Messaging services for in-scope agencies are currently located in 54 separate messaging systems on a variety of different platforms:
  - Exchange 2000, 2003 (34 systems,)
  - Exchange 5.5 (2 systems)
  - Notes (1 system)
  - Groupwise (12 systems)
  - Sendmail/Pop3/Other (5 systems)
- Some mail systems host multiple agencies
- No unified email directory
- Most mail sent from agency to agency over the internet

Requirements for Exchange and Adjunct Services

- Messaging for in-scope agencies services must be moved to one centralized enterprise messaging infrastructure located in CESC
- Must support one common email directory through Active Directory
- Messages must be sent from agency to agency within the enterprise network
- Must support current adjunct messaging services such as Public Folders, Blackberry, instant messaging, team workspaces, unified messaging as well as services such as mail encryption and journaling
- Must support messaging SLAs
- Must support SLAs for failover

Messaging Vision



Timeline for Exchange and Adjunct Services

- We are working with three significant timeframes:
  - Timeframe 1: Now until CESC is ready (Fall 2006 to June 2007)
    - Shared Messaging environment in the RPB being leveraged to supply AD forest and Exchange Organization for eventual enterprise messaging system
    - Some limited changes made to AD to support directory synchronization in this period
  - Timeframe 2: CESC Ready (June 2007 to July 2007)
    - New messaging infrastructure in CESC built out and ready to support users
  - Timeframe 3: SWESC ready (November 2007 to December 2007)
    - SWESC built out, infrastructure for failover in place and processes for failover complete

Exchange and Adjunct Services Implementation

- What this means, functionally:
  - For timeframe 1 (now until CESC is ready):
    - Alter the existing Shared Messaging (“COV”) environment to support transformation objectives
    - Lay the foundation for timeframe 2 activities where possible
  - For timeframe 2 (after CESC is ready):
    - Deploy a “new” Exchange and Adjunct Services environment capable of supporting all requirements
    - This essentially involves deploying a “Greenfield” Exchange and adjunct services architecture implemented in parallel to the COV architecture (and temporarily incorporating the COV architecture)

Why Not Just Adopt the COV?

- There are many reasons; these include:
  - AD/Exchange originally designed with certain principles and objectives in mind. Some of the messaging architectures and features that AD must support do not fit into the confines of those principles.
  - Not all required services are present.
  - Insufficient capacity – current AD and Exchange capacity represents only a small fraction of what is needed.
  - Deployed architecture cannot be easily changed without impacting production users. (E.g. single active/active Exchange cluster cannot be expanded).

Solution Overview

- Based on Exchange 2003 and Windows 2003 Active Directory
  - Support for remote access through OWA and rpc/https
  - PKI infrastructure to support encrypted mail
  - Journaling of mail as required by agency
- Centralized Adjunct Messaging Services:
  - Blackberry
  - Sharepoint Portal Services for team workspaces and to replace Public Folders wherever possible
  - Instant Messaging within the enterprise network through Live Communication Server
  - Integrated Fax Services
  - Unified Messaging
- Replication of data to SWESC for failover of services

High Level Design Elements

- Exchange 2003 Logical Elements
  - One Exchange Organization
  - One Exchange Routing Group
  - Current smtp email addresses migrated, no new addressing scheme
  - SMTP addresses will be stamped by MIIS which will remain in place after transformation is complete
  - Exchange servers located in their own AD site in CESC to segment directory server authentication and directory lookup traffic
  - All mail screened at smtp gateway for viruses and spam

High Level Design Elements Cont.

- Exchange 2003 Physical Elements
  - All mail servers located centrally in CESC
  - Exchange on blade servers
  - Mail storage servers in 3a\1p node clusters
  - Mail data stored on SAN system
  - Designed to be scalable, initially scaled to support current users

High Level Design Elements Cont.

- Adjunct messaging
  - Blade servers used
  - Designed to be scalable, initially scaled to support current users of each service

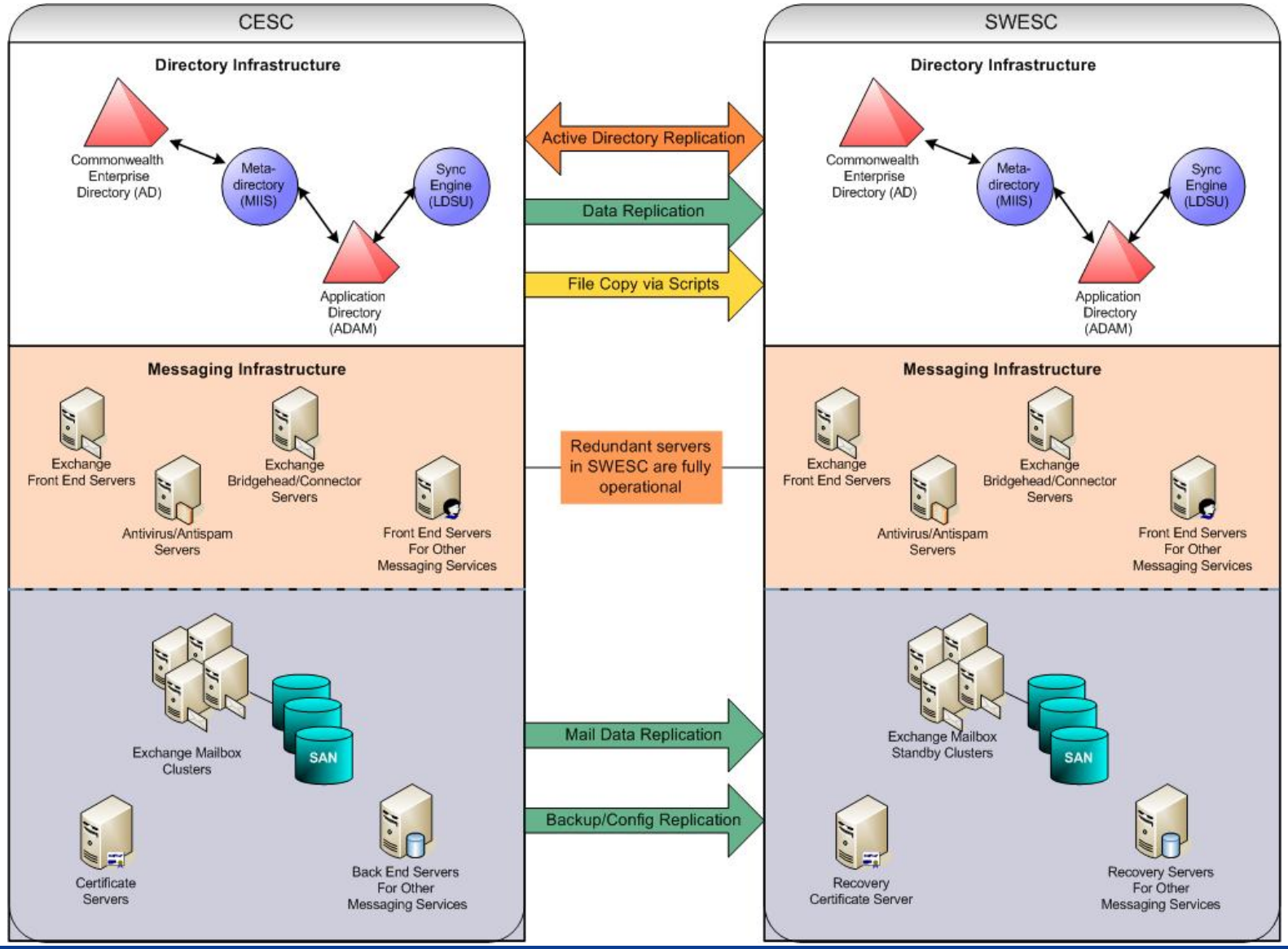
Exchange Hardware and Software

- Exchange Software
  - Windows 2003 Active Directory
  - Windows 2003 Server sp2
  - Windows Exchange Server 2003 sp2
- Hardware
  - A hardware profile utilizing blades has been created for various Exchange Server roles
    - Mailbox
    - Bridgehead
    - Front End

Adjunct Services Software\Hardware

- Software
  - Support built into Exchange 2003 and AD for
    - Encrypted mail
    - Journaling
    - Public Folders
  - Blackberry Wireless Services for Wireless Support
  - Sharepoint Portal Server for collaboration and workgroup functionality
  - Live Communication Server for Instant Messaging Services
  - Fax Solution – TBD - Dependant on existing agency services and licenses
  - UM – TBD - Dependant on existing agency services and licenses
- Hardware
  - Will be hosted on Blade hardware

Site Failover



Interface to Existing Solutions

- Existing separate email directories are synched prior to buildout of new centralized enterprise system
- Synch continues throughout migration between migrated and unmigrated agencies
- Email is exchanged via smtp during coexistence phase either within the internal network or over the internet
- As agency is migrated, DNS MX record is redirected to the new system.

User Interaction

- Exchange
  - Outlook 2003 email client is the standard Exchange 2003 client. Outlook is currently used by most users
  - Users will also have OWA and rpc\http access
- Sharepoint Portal Server access is through a web browser
- Instant messaging supported through Windows Messenger or Office Communicator clients
- Current Blackberry devices supported for wireless connectivity
- UM and Fax server software to be determined but access to fax and voicemail will be available through Outlook and Exchange

Dependencies

- CESC and SWESC buildouts
- Agency must have received new desktops or desktop image prior to migration
- Agency workstations must have Altiris agents loaded
- Agency must be connected to new enterprise network prior to migration

Questions

NORTHROP GRUMMAN

Active Directory
High Level Design Review

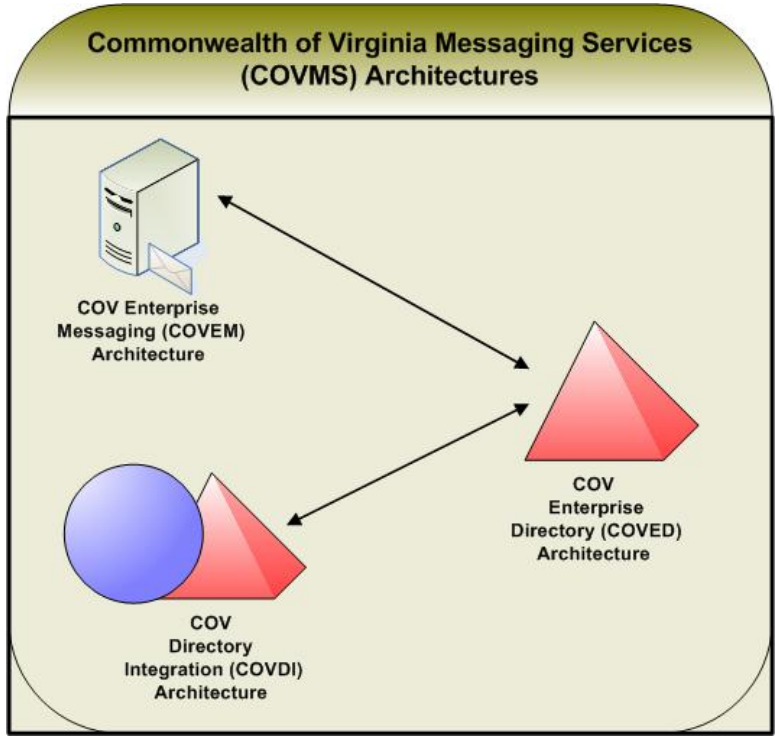
Agenda

- Introduction
- Requirements and Vision for Active Directory
- Timeline for Active Directory
- Solution Overview
- Solution Hardware and Software
- Implementation Plan
- Interfaces to Existing Solutions
- Affect on User Population
- Dependencies
- Risks

Introduction

Messaging Tower Tracks:

- Exchange – Messaging and Adjunct Services (Mobile, IM, Unified Messaging, Fax)
- Directory Synchronization – MIIS, LDSU, and other products provide a common GAL and a unique identifier for users. Also lays some groundwork that would be necessary to support other services in the future

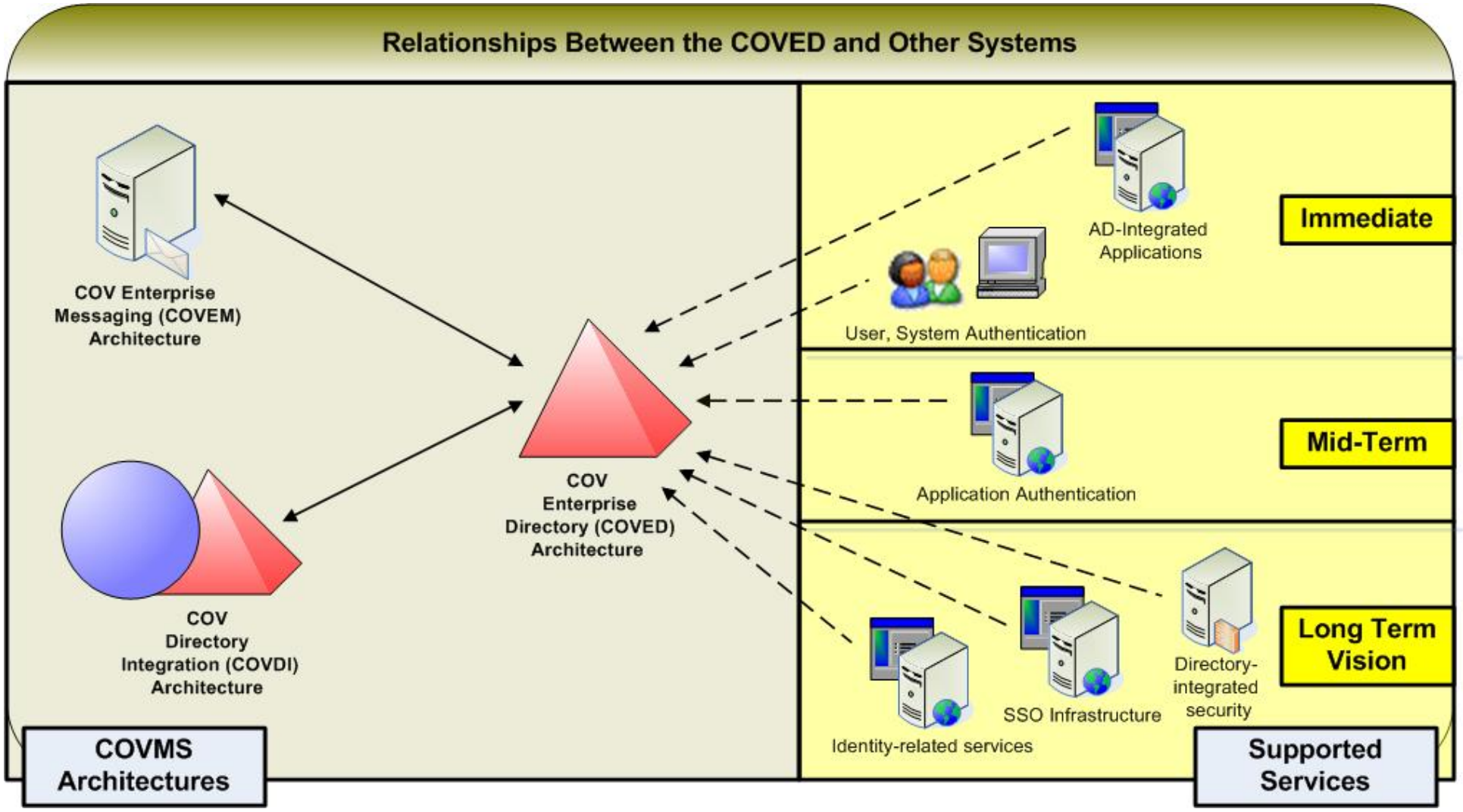


- **Active Directory** – Windows 2003 AD to provide an enterprise directory, single source for authentication, etc. Also, DNS, WINS, and related services
- Migration – how are users and mailboxes in agency directories and email systems going to transition to the new messaging infrastructure?

Requirements for Active Directory

- New Active Directory architecture will be of critical importance to VITA both short term and long term
  - Must support Exchange and adjunct services (mailboxes, users, groups, accounts for 67,000 users)
  - Must support the Directory Synchronization effort
  - Must support migrated workstation authentication
  - Must support Northrop Grumman's transformation plan for the Commonwealth of Virginia administratively
  - Must support the directory services needs of applications required by other functional areas (e.g. OpenView, Altiris, etc.).
  - From a vision and best practices perspective, should support un-scoped but foreseeable potential future uses (e.g. target for application authentication, application standardization, identity management, single sign-on, etc.)

Vision for Active Directory



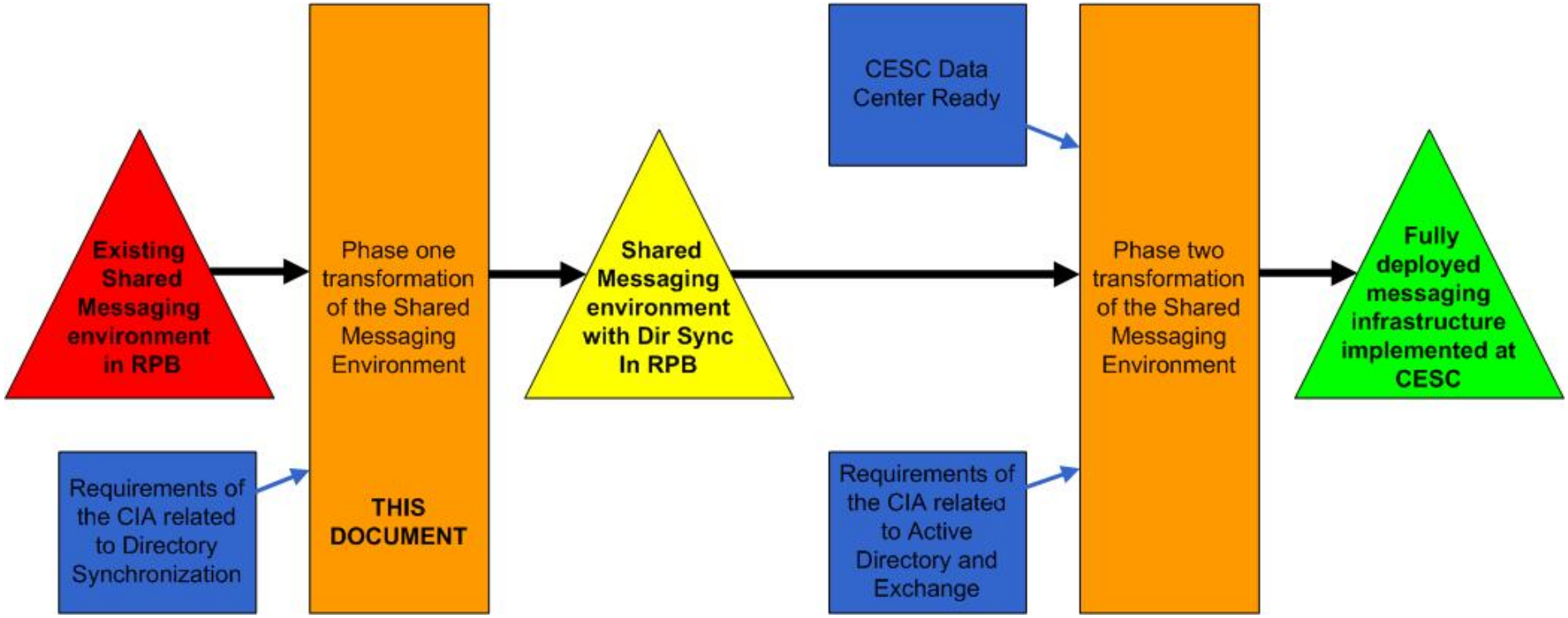
Timeline for Active Directory

- We are working with three significant timeframes:
  - Timeframe 1: Now until CESC is ready
    - AD objectives for timeframe 1: support directory synchronization effort and application requirements of other functional areas (Altiris, OpenView, etc.)
  - Timeframe 2: CESC ready until migrations complete
    - Active Directory objectives for timeframe 2: deploy an AD architecture capable of fully complying with requirements
  - Third timeframe: SWESC ready
    - Active Directory objectives for timeframe 3: support additional layer of failover capabilities

Active Directory Implementation

- What this means, functionally:
  - For timeframe 1 (now until CESC is ready):
    - Alter the existing Shared Messaging (“COV”) environment to support pre-CESC transformation objectives
    - Lay the foundation for timeframe 2 activities where possible
  - For timeframe 2 (after CESC is ready):
    - Deploy a “new” Active Directory environment capable of supporting all requirements
    - This essentially involves deploying a “Greenfield” AD architecture in CESC (and temporarily incorporating the COV architecture); systems will be joined to COV
  - For timeframe 3 (SWESC is ready):
    - Addition of domain controllers and sites to support failover

COV Transformation Approach



Why Not Just Adopt the COV?

- There are many reasons; these include:
  - AD/Exchange originally designed with certain principles and objectives in mind. Some of the messaging architectures and features that AD must support do not fit into the confines of those principles.
  - Not all required services are present.
  - Insufficient capacity – current AD and Exchange capacity represents only a small fraction of what is needed.
  - Deployed architecture cannot be easily changed without impacting production users. (E.g. single active/active Exchange cluster cannot be expanded).

Solution Overview

- Logical Elements
  - Will be designed to reflect the administrative model
  - Implemented design will help to make management intuitive and secure
  - Logical elements of design are items such as forest / domain model, organizational unit structure, etc.
- Physical Elements
  - Physical elements of design are items such as subnet/network layout, and domain controller configuration / placement
  - Will be designed to reflect the physical layout of AD
  - Implemented design will help to ensure service availability and directory services performance; also enhances end user experience.

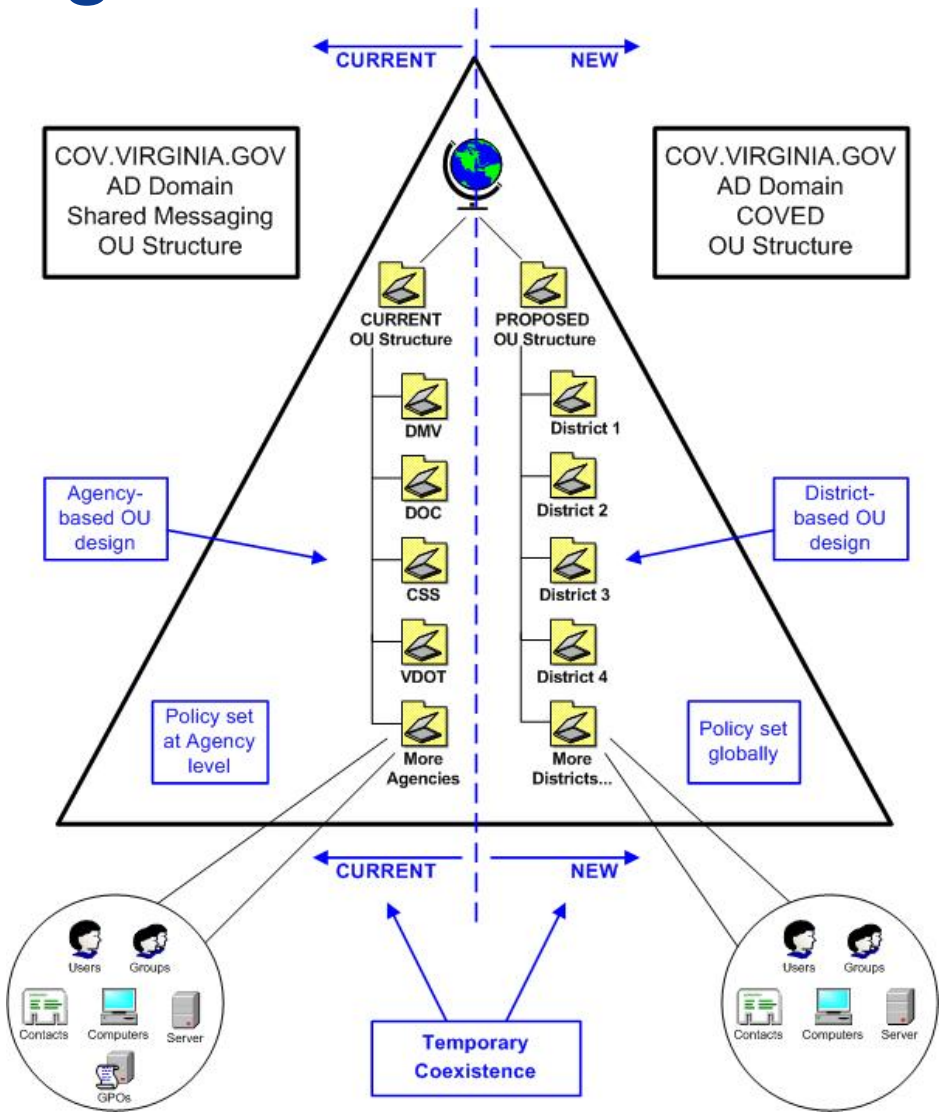
Logical Element Design

- Forest and Domain Model
  - Best practice for Active Directory design in this scenario is single forest and single domain. Best for support of new administrative model.
  - Additional domains can be added later if a business need arises
  - Same configuration as Shared Messaging environment
- Organizational Unit (OU) Design
  - Reflects how the forest/domain is administered.
  - New administrative model calls for all users in the Commonwealth of Virginia to be supported by a single administrative structure, however some types of services will be managed regionally.
  - Therefore, OU structure is based on regions, not Agencies
  - Additional OUs will support centralized infrastructure (enterprise production and enterprise failover) as well as external service delivery when appropriate

Organizational Unit Design

Differences between old OU structure and new OU structure:

- Old structure (left side of graphic) for Shared Messaging environment based on Agency.
- New structure (right side of graphic) based on districts (regions)



Logical Element Design

- Group Policies
  - Allow control over settings on users and/or computers in Active Directory.
  - Group policies will be put in place where necessary to support administration of users and devices, but specific policies have not yet been defined
  - In the Shared Messaging environment, group polices are also used to deploy applications, however in the new environment Altiris will handle this function.

Physical Element Design

- Active Directory Site Design
  - Tells AD which domain controllers should provide authentication services to which systems, based on their network address
  - In the new administrative model, the structure is essentially flat because all services are delivered centrally
  - Therefore, a single site will hold all domain controllers (except those for Exchange and failover support).
  - Exchange is a special case. It is directly dependent upon Active Directory and places a specific, predictable load on the directory service.
  - To ensure that Exchange is not competing with users and devices attempting to authenticate, it will have a dedicated site and domain controllers.
  - When SWESC is available, some domain controllers will exist in the failover location, but will not be utilized unless a failover event occurs.

Physical Element Design

- Global Catalog Services
  - Global catalog (GC) servers are a special kind of domain controller. They hold a copy of the “important attributes” for all objects in the forest.
  - If a domain controller is not a GC, then a separate GC must be contacted during authentication to complete the process
  - In a single forest, single domain model, best practice calls for all domain controllers to be configured as global catalog servers.
  - All deployed domain controllers to be configured as global catalog servers. System documentation will indicate that all domain controllers deployed in the future be configured as global catalog servers.

Physical Element Design

- Flexible Single Master Operations (FSMO) Roles
  - Active Directory mostly works in multi-master fashion
  - However some functions cannot be multi-master due to their nature. These “single master” roles are held by one domain controller at a time.
  - Forest FSMO roles: Schema Master, Domain Naming Master
  - Domain FSMO roles: RID Master, PDC Emulator, Infrastructure Master
  - In the Shared Messaging environment, all roles are held on a single domain controller.
  - In the new COVED, post-CESC, forest related FSMO roles will be held on one DC and domain related FSMO roles will be held on a second. This will be done to (1) spread the increased workload, and (2) minimize short term impact associated with a FSMO DC outage

Other Design Elements

- Time Synchronization
  - By default, all domain controllers get their time from the PDC Emulator FMSO role server.
  - All other servers and workstations get their time from the DC that authenticated them.
  - To ensure that the PDC Emulator maintains accurate time, it will be pointed to an external time source (either an atomic clock on the Internet or an internal network device that gets its time from an external source). Exact source TBD.
- Active Directory Operating Modes
  - AD is capable of operating in sever “modes”, each of which provides a slightly different set of features and/or supports different types of domain controllers participating in replication
  - As legacy domain controller support is not necessary, the operating mode of AD will be set to the “Windows 2003” level (both forest and domain)

Other Design Elements

- Trust Relationships
  - Trust relationships establish a security relationship between directory services
  - Essentially, they instruct one directory service to “trust” users authenticated by a second directory service and typically allow those users to access resources in the domain where they did not directly authenticate.
  - Trust relationships can be used in many ways…
    - Short term and during the migration effort, trust relationships may be established to agency directory services to smooth the migration effort.
    - Mid-term and after migration effort, it may be necessary to keep some trust relationships in place to allow migrated users to easily access legacy resources.
    - Long term, trust relationships should not be necessary.

Hardware and Software

- Software
  - Windows 2003 Active Directory
  - Windows 2003 Server
- Hardware
  - A standard hardware profile has been created for a domain controller.
    - Single or dual CPU, 2 GB RAM, 2x36 GB drives in a RAID 1 configuration
  - Physical server counts, mapping to sites, and hardware specifications will be defined in later documents
  - Scaling for user and Exchange support per best practices (8,000 user per GC & 1 GC for every 4 Exchange CPUs)

Implementation Plan

- Three Phases of Effort:
  - Phase 1 – pre-CESC
    - Leverage the Shared Messaging environment, but modify it to support the Directory Synchronization architecture and cross-functional area application needs
    - High level list of changes:
      - Process changes for change control
      - Parallel OU structure
      - Administration allowed for parallel OU structure
      - Additional domain controller
      - Addition of Directory Synchronization architecture

Implementation Plan

- Three Phases of Effort:
  - Phase 2 – CESC
    - Deploy a parallel architecture and infrastructure capable of meeting the requirements of the CIA
    - Essentially this will be a “Greenfield” Active Directory built on the cov.virginia.gov forest/domain
    - Existing COV OU structure and sites remain in place pending migration of in-scope entities and determination regarding service continuation for out-of-scope entities
  - Phase 3 – SWESC
    - Additional failover capabilities added

Interfaces to Existing Systems

- Phase 1 effort extends the capabilities of the Shared Messaging environment, therefore changes are:
  - Support for the directory synchronization architecture
  - Support for Altiris, OpenView, and any other cross-functional area applications or service dependencies (DNS, WINS, etc)
- Phase 2 effort will involve:
  - Deploying a new Active Directory architecture
  - Integrating the new Exchange architecture into the Active Directory architecture
  - Migrating the Directory Synchronization architecture in RPB to CESC, integrating it into the new environment
  - As users are migrated will begin authenticating to the new architecture

Interfacing with Active Directory

- It is expected that many towers will have AD-requirements or dependencies.
- These are expected to fall into four general categories:
  - Directory-integrated COTS applications require basic rights in the directory service or schema extensions to the directory
  - Directory-dependent custom applications require custom schema object/attribute creation and rights
  - Applications or services will require rights to objects in Active Directory to manage the objects.
  - Applications will want to manage and monitor Active Directory components.
- We will develop processes for each scenario and others that emerge.

Affect on User Population

- As all in-scope users will eventually reside in the new Active Directory architecture, all users will eventually be affected.
- But… the migration of users from their current directory service to the new AD architecture - not the introduction of the architecture itself - would create end user impact.

Dependencies

- For Phase 2:
  - CESC readiness
  - Connectivity between RPB Shared Messaging environment and CESC for the purpose of establishing and maintaining AD replication
  - Hardware availability
  - Network readiness (impacts migration)
  - Lab readiness

Risks

- Changing a production environment (Shared Messaging environment) has limited potential to impact production users
- Getting architecture in place may be slowed because we will be expanding a production system rather than working completely “Greenfield”
- CESC and network readiness

Questions